Exhibit P

ANDREW CRAIN REBUTTAL REPORT

I. Background

1. On July 1, 2021, I provided the Andrew Crain Expert Report (the "Crain Report"), in conjunction with the prosecution's engagement of Berkeley Research Group ("BRG") in this matter. For background, I was asked to provide in the Crain Report various opinions related to the forensic analysis that my team and I performed on digital forensic evidence provided for our review.

2. On September 10, 2021, Jinhua's disclosed expert in this matter, Mr. John Ashley, provided a disclosure statement of opinions and observations (the "Ashley Disclosure").

3. I am providing this rebuttal report in response to certain points raised in the Ashley Disclosure.

II. Summary of Rebuttal Opinions

4. The opinions I provided in the Crain Report are largely unchanged in response to the Ashley Disclosure because, at the highest level, the Ashley Disclosure did not address my findings concerning the copying and opening of numerous charged trade secret documents in this matter. Instead, the Ashley Disclosure suggested that, because some evidentiary computing devices were used after the devices were seized—and therefore certain limited evidence on those devices underwent changes— those evidentiary datasets are now unreliable. I do not agree.

5. As described more fully in the following sections, the Ashley Disclosure:

    a) Does not allege that any post-seizure access occurred whatsoever for five specific evidentiary datasets which, as described in the Crain Report, contain forensic evidence indicating copying and/or opening of all but two of the charged trade secret documents in this matter;
    b) Does not identify even a single instance in which post-seizure access rendered unreliable the forensic evidence underpinning a pre-seizure event described in the Crain Report;
    c) Identified only a single instance of a charged trade secret document being opened post-seizure.

6. Accordingly, I do not believe the post-seizure access to some of the datasets at issue, as described in the Ashley Disclosure, impacted in any way the reliability of the forensic evidence described in the Crain Report. In fact, because the post-seizure access described in the Ashley Disclosure was captured in the available metadata, and is therefore reliable in the same fashion as the data and metadata described in the Crain Report, we can be highly confident that the post-seizure access had no effect on the pre-seizure forensic evidence outlined in the Crain Report.

7. I reserve the right to amend, alter, or supplement my findings should additional evidence / information be provided to me for analysis, or to rebut testimony from defense witnesses. I also reserve the right to create demonstratives for use at trial and / or to use other graphical depictions to present my findings.

III. Post-Seizure Access to Some of the Original Data Sources Did Not Have Any Impact on the Specific Forensic Evidence Indicating the Pre-Seizure Copying and Opening Events Detailed in the Crain Report

8. The Ashley Disclosure details at length its findings related to the fact that some, but not all, of the original data sources in this matter were accessed after the date on which they were seized by Taiwanese law enforcement. But notably, as discussed more fully below, only one charged trade secret document was accessed (on a single occasion) during this post-seizure access.

9. As a general matter, I agree that proper handling of digital evidence is important, and that litigants and law enforcement personnel should strive to follow best practices with respect to the preservation and examination of digital forensic evidence. It is also a common, practical reality in the digital forensics industry, however, that original sources of digital evidence have not always been preserved in strict accordance with such best practices. As a result, certain forensic information contained in those datasets (such as date / time stamps) can be inadvertently or unwittingly changed prior to forensic imaging and examination.

10. In such instances, forensic examiners can analyze and rely on specific forensic artifacts contained within those datasets that were unaffected by such later events, and hence, remain accurate as to what occurred before. Specifically, regarding the instant matter, the post-seizure access to some of the original data sources did not affect, let alone destroy, copious and reliable forensic evidence of pertinent events on those devices that occurred *prior* to seizure. In fact, all the forensic evidence cited in the Crain Report related to pre-seizure copying and opening of the charged trade secret documents on the various devices remains unchanged by the post-seizure access described in the Ashley Disclosure. And with one minor exception unrelated to post-seizure access, the Ashley Disclosure asserts no opinion to the contrary.[1]

11. In fact, the Ashley Disclosure identified only a single instance in the Crain Report of a file opening corresponding to a charged trade secret document that occurred post-seizure (i.e. the February 13, 2017 opening of trade secret document number 5 on the BRG009 device).[2] Additional forensic evidence from the BRG009 device confirms, however, that the underlying

[1] Separate from his contentions relating to post-seizure access, the Ashley Disclosure discusses (at pp. 25-26) a specific timestamp that occurs on the BRG010 device as a possible result of a failing internal battery, causing the system clock on that device to reset to 1/1/2003 (or 12/31/2002 subject to a time-zone offset). I agree that this date stamp – 12/31/2002 – is unlikely to reflect the actual date and time of the associated event. Mr. Ashley does not assert or even suggest, however, that any of the 12/31/2002 timestamps occurred *after* seizure of BRG010. Indeed, Mr. Ashley does not assert that any post-seizure access occurred at all with respect to the BRG010 device. Furthermore, I disagree with Mr. Ashley's supposition that this occasional system clock reset due to battery failure "cause[s] all time and date metadata on the hard drive [of BRG010] to be unreliable" (Ashley Disclosure, p. 26). The Ashley Disclosure appears to then concede this point (at pp. 26-28), where it identified only 12 items from BRG010 with the date of 12/31/2002, rather than all items originating from the BRG010 source (*see, e.g.*, Crain Report Exh. D, reference nos. 59, 63, 546, 565-66 (among others) (identifying other events tied to the BRG010 device with date stamps other than 12/31/2002 and which Mr. Ashley does not identify as being "incorrect dates" [Ashley Disclosure, p. 26]).

[2] *See* Ashley Disclosure, pp. 21-22; *see also* Crain Report at ¶ 21(k).

document was not modified during this opening event.[3] That is, the evidence shows that on that date, the document was opened on BRG009 and then closed, without making or saving any changes.

12. In paragraph 4 of the Crain Report, I identified the various artifacts that my team and I used to reach the conclusions in that report. Each of those artifacts was unaffected by the post-seizure events that occurred later. This is critical because it means that the conclusions in the Crain Report are unaffected by the contentions of post-seizure access in the Ashley Disclosure. For example:

    a) File system created dates, link file created dates, and Office Alerts are not subject to modification by later events, and therefore can be relied-upon despite subsequent access to the device.

    b) Generally speaking, the file system last modification date for link files could be updated by later events (i.e., if the document in question was opened again). Yet none of findings in the Crain Report relating to the charged trade secret documents were affected by post-seizure updates to link file last modification date / time stamps.[4]

    c) The Windows jumplist artifact, akin to a ledger of files opened in the past, similarly is intact; it may show 'new' entries or show an updated embedded "last accessed" value for files opened on a device post-seizure, but none of the events relating to charged trade secret documents described in the Crain report were affected by a post-seizure entry or update in the Windows jumplist artifact.

13. Many forensic artifacts, including all the evidence relied upon in the Crain Report, provide a reliable and accurate historical record of file copying and opening. They are not overwritten or changed when other unrelated events occur on the computer. Indeed, the Ashley Disclosure itself actually confirms this -- a substantial portion of the Ashley Disclosure is dedicated to cataloging multiple events that occurred between the seizure and the forensic imaging of the evidentiary devices. The very fact that the Ashley Disclosure can conclude that some events (such as file copying, file opening, and file deletions) occurred post-seizure, irrespective of the fact that still other events occurred *even later* in time,[5] confirms that the mere existence of forensic artifacts on a computer after a particular event does not invalidate or render any less reliable the forensic evidence of previous events on that computer. Put simply, the later events *add* to the history, rather than delete or change prior history.

---

[3] The file system last modification date for this document, as stored on the BRG009 device at the folder path: /Documents and Settings/Administrator.KENNY/桌面/USB/90s/V90B/0. Design/EES Document/【DR25nmS】Design rules Periphery_EES_2012000026-013_Rev.13.xls, remains May 5, 2016. This indicates the document was not substantively modified during the opening event on February 13, 2017.

[4] The February 13, 2017 opening of Trade Secret 5 on BRG009 (*see, e.g.* Crain Report at ¶ 21(k)) was based on link file evidence that was created and modified on that date, versus created earlier and then updated on that date.

[5] *See, e.g.*, Ashley Disclosure, pp. 8-10, describing a chronology of events on BRG003 spanning multiple days post-seizure, including specific events of machine access, copying, USB insertion, and file opening.

14. In sum, the Ashley Disclosure does not identify a single instance in which post-seizure access rendered unreliable any of the forensic evidence underpinning pre-seizure findings described in the Crain Report.

IV. The Ashley Disclosure Makes No Mention of Any Post-Seizure Access to Five Datasets Identified in the Crain Report that Contain Evidence of Copying and/or Opening of Virtually All the Charged Trade Secret Documents

15. The Crain Report details forensic evidence from five datasets (BRG008,[6] BRG010,[7] BRG026,[8] BRG027,[9] and BRG028[10]) that shows copying and/or file opening events related to all but two of the charged trade secrets documents (i.e., numbers 1 (documents 4-16), 2, 3, 4, 5, 6, 7, and 8). The Ashley Disclosure makes no mention of any post-seizure access to any of these five datasets. Accordingly, as these datasets are not challenged by Mr. Ashley, I am not addressing them further.

V. The Ashley Disclosure Discusses Post-Seizure Access on Four Datasets For Which the Crain Report Asserts No Findings About Copying or Opening of Charged Trade Secrets

16. The Ashley Disclosure asserts that that data access occurred post-seizure on, among others, BRG004,[11] BRG006,[12] BRG023,[13] and BRG024.[14] The Crain Report offered no substantive opinions as to the existence or use of charged trade secrets on any of these devices. Accordingly, I am not addressing these devices further.

VI. Several Devices Discussed in the Ashley Disclosure as Being Accessed Post-Seizure Actually Show Only a Small Number of Non-Substantive, Automatic Updates, or Other Updates Not Germane to the Findings in the Crain Report

17. The Ashley Disclosure discusses that the BRG011, BRG013, and BRG014 datasets were subject to a small number of files being "created and then deleted"[15] on each device after seizure and prior to forensic imaging. This discussion leaves the reader with the impression that investigators were, for example, adding new substantive files to the devices, or were deleting substantive, user-

[6] *See, e.g.*, Crain Report, ¶¶ 16-17 and corresponding footnote(s).
[7] *See, e.g.*, Crain Report, ¶¶ 16-17 and corresponding footnote(s).
[8] *See, e.g.*, Crain Report, *passim.*
[9] *See, e.g.*, Crain Report, ¶ 15 and corresponding footnote(s).
[10] *See, e.g.*, Crain Report, *passim.*
[11] *See, e.g.*, Ashley Disclosure, pp. 11-12.
[12] *See, e.g.*, Ashley Disclosure, pp. 12-13.
[13] *See, e.g.*, Ashley Disclosure, pp. 19-20.
[14] *See, e.g.*, Ashley Disclosure, pp. 20-21.
[15] The Ashley Disclosure identifies thirty-one (31) such files for BRG011 (Ashley Disclosure at pp. 15-16 and Exh. 13), one (1) such file for BRG013 (Ashley Disclosure at pp. 17-18 and Exh. 16), and seven (7) such files for BRG014 (Ashley Disclosure at pp. 18-19 and Exh. 17).

generated files[16] ("User Documents") present on the device, thereby introducing confusion as to what data was on the device as attributable to custodial actions. However, no such confusion exists because the post-seizure actions are readily identifiable by their metadata—as is evident from the Ashley Disclosure's discussion and numerous exhibits detailing exactly those actions. In addition, the Ashley Disclosure critically fails to mention that the file creations and deletions on each of these three datasets occurred automatically, as a result of simple file opening activity and thus relate only to a small number of non-substantive files.

18. More specifically, the files that were created and deleted from the BRG011, BRG013, and BRG014 datasets after seizure are referred to as "Office owner" files, which I discussed in the Crain Report at paragraph 2.b. "Office owner" files are small temporary files which are automatically created by Microsoft Office when an Office document is opened on a computer. "Office owner" files follow the naming convention of prepending "~$" to the filename of the Word, PowerPoint, Excel, etc. file being opened, and the "Office owner" file is then automatically deleted by the computer when the underlying Office document file is closed. "Office owner" files serve to 'lock' the underlying file so that only one user can make changes at a time, to avoid data conflicts with simultaneous editing.

19. Thus, while it is true that BRG011, BRG013, and BRG014 show evidence (via these "Office owner" files) of file opening after the devices were seized, none of the "file creations or deletions" identified in the Ashley Disclosure resulted in the addition or modification of any User Documents on any of these devices. Similarly, these post-seizure "file creations and/or deletions" did not cause the deletion of any User Documents that were already on the devices when seized.

20. Finally, the Ashley Disclosure's discussion regarding other evidence of post-seizure access on BRG013 pertains only to the "last modification" date of folders—not any of the User Documents therein—or to automatic system artifacts that record file system transactions on the computer.[17] These items are also simply the automatic effects of file browsing/opening activity and did not affect the underlying substantive data on the dataset. Furthermore, these alterations would not affect—nor does the Ashley Disclosure allege that they would—any of the findings in the Crain Report with respect to these datasets.

VII. With a Single Exception, the Post-Seizure Access to Three Devices Discussed in the Ashley Disclosure Had Nothing to Do With the Charged Trade Secret Documents in This Matter

A. Post-seizure access to the datasets BRG003, BRG009, and BRG012 did not affect the reliability of the forensic evidence on those devices related to pre-seizure events, and only one post-seizure access had anything to do with the charged trade secret documents on those devices, as detailed in the Crain Report.

[16] As used here, I am referring to a category of document types that users typically create, modify, and/or review during their work on the devices, as distinct from the many operating system and application type files also contained on the devices. "User Documents" includes, for example, Microsoft Office files (such as Word, PowerPoint, Excel), as well as PDF files, emails, etc.

[17] *See* Ashley Disclosure, Exh. 16.

21. The Ashley Disclosure details various post-seizure access to three datasets—BRG003, BRG009, and BRG012—including files and folders being created and deleted on those devices.[18] As described earlier, however, none of this post-seizure activity had any effect on the reliability or accuracy of the forensic evidence, as described in the Crain Report, showing that each of these devices had been used prior to seizure to copy and/or access to charged trade secret documents.[19]

22. Moreover, for all of the post-seizure access described in the Ashley Disclosure, Mr. Ashley points to only a single instance of a single charged trade secret document which was impacted in any way -- when charged trade secret number 5 was opened on February 13, 2017 on the BRG009 device.[20] Furthermore, that single event was solely an opening event—the substantive content of charged trade secret number 5 on BRG009 was not changed in any way on February 13, 2017.[21]

23. Stated differently, of the more than 180 specific events detailed in the Crain Report[22] involving copying or opening of charged trade secret documents, the Ashley Disclosure points out that only one of those events took place after the subject devices were seized, and the forensic evidence establishes that that event did not change the actual content of the file involved.

24. In addition, closer analysis of the other files and folders whose date/time stamps were updated during post-seizure access reveals a somewhat different story than what the Ashley Disclosure leads the reader to believe. For one device, BRG003, more than 93% of the files which were created during post-seizure access were the result of Taiwanese MJIB saving a copy of a network share at UMC to the device.[23] For the other two devices, BRG009 and BRG012, all of the files and folders that were created post-seizure consist solely of system-type files (not User Documents), and created automatically via booting and operation of the computer.[24] And for all three devices, all of the files and folders that the Ashley Disclosure asserts were deleted during post-seizure access consist entirely of temporary and system files, rather than User Documents.[25]

---

[18] *See, e.g.*, Ashley Disclosure, pp. 8-11 and Exh. 6 (relating to BRG003), pp.13-15 and Exh. 11 (relating to BRG009), pp. 16-17 and Exh. 14 (relating to BRG012).
[19] *See, e.g.*, Crain Report, pp. 11-12 (detailing evidence on the BRG003 device regarding charged trade secret documents 5, 6, and 7), pp. 7-13 (detailing evidence on the BRG009 device regarding charged trade secret documents 1 (numbers 2, 3, 6, 8-16), and 2-8), and pp. 8-13 (detailing evidence on the BRG012 device regarding charged trade secret documents 1 (numbers 4-7, 10-16) and 5-8).
[20] Discussed above in ¶ 11.
[21] The file system last modification date for this document, as stored on the BRG009 device at the folder path: /Documents and Settings/Administrator.KENNY/桌面/USB/90s/V90B/0. Design/EES Document/【DR25nmS】Design rules Periphery_EES_2012000026-013_Rev.13.xls, remains May 5, 2016. This indicates the document was not substantively modified during the opening event on February 13, 2017.
[22] *See* Crain Report, ¶¶ 11-25.
[23] *See* Ashley Disclosure, pp. 8-11 and Exh. 6.
[24] *See* Ashley Disclosure, Exhs. 11, 14.
[25] *See* Ashley Disclosure, Exhs. 6, 11, 14.

25. The below chart summarizes the more detailed context of the post-seizure access on the BRG003, BRG009, and BRG012 datasets:

Events During Post-Seizure Access	BRG003[26]	BRG009[27]	BRG012[28]
Files/Folders Created Post-Seizure	34,905	91	160
Files/Folders Created Due to UMC Network-Share Download Post-Seizure	32,688 (> 93%)	0	0
System/Temporary Files/Folders Created Post-Seizure[29]	2,100+	91	160
Files/Folders Deleted Post-Seizure	1,267	15	21
System/Temporary Files/Folders Deleted Post-Seizure	1,267	15	21
Charged Trade Secret Files Created Post-Seizure	0	0	0
Charged Trade Secret Files Modified Post-Seizure	0	0	0
Charged Trade Secret Files Deleted Post-Seizure	0	0	0

B. The Ashley Disclosure alludes to potential spoliation of evidence owing to post-seizure access, yet fails to identify any forensic evidence that was lost, or was likely to have been lost, and which may have been helpful to Defendants

26. The Ashley Disclosure repeatedly asserts that post-seizure access amounts to a loss of relevant evidence on various devices.[30] With respect to one device – BRG003 – the Ashley Disclosure points out that significant data volume was added post-seizure, and that this newly added data may have overwritten previously-existing data within that storage space.[31] While this is correct from a technical standpoint, the Ashley Disclosure cites no forensic evidence indicating that any data was actually lost, nor does the Ashley Disclosure attempt to identify what type of data may have been lost that would have been pertinent to his forensic examination or would otherwise bear on the findings in the Crain Report. Again, it also did not impact any of the charged trade secret documents, as depicted in the chart above.

//

//

[26] *See* Ashley Disclosure, p. 8 and Exh. 6.
[27] *See* Ashley Disclosure, p. 13 and Exh. 11.
[28] *See* Ashley Disclosure, p. 16 and Exh. 14.
[29] The BRG003 device contains approximately 15-20 User Documents that were created post-seizure in the "Desktop" folder of Mr. Wang's user profile (46685), and which were not part of the download of the "NBD" UMC network share. *See also* Ashley Disclosure, Exh. 6.
[30] *See* Ashley Disclosure, pp. 7-8, 11, 20, 21. As discussed earlier, however, the post-seizure effects for numerous of the evidentiary devices pertained to either a small number of non-substantive "Office Owner" files, or to devices about which the Crain Report asserted no findings.
[31] *See, e.g.*, Ashley Disclosure, pp. 7-8, 11, 31-32.

VIII. Excluding Post-Seizure Opening Events From the 'Company' Embedded Metadata Analysis Described in the Crain Report Still Shows Hundreds of File Openings Before The Devices Were Seized

27. The Crain Report detailed certain forensic evidence showing that files responsive to specific criteria (such as a particular value in the "company" embedded metadata field or containing the phrase "Micron confidential") were opened on various devices.[32] The Ashley Disclosure discussed that some of these file opening events occurred either post-seizure, or in the case of the BRG010 device, were associated with date / time stamps from 2002.[33]

28. Even excluding the post-seizure and 2002 events discussed in the Ashley Disclosure, the forensic evidence in this matter clearly shows that hundreds of document instances were opened that meet either/both these criteria. With these exclusions, the numbers in the Crain Report can be revised as follows:

    a) Crain Report, paragraph 7: This analysis determined that at least 439 document instances in the evidentiary population were: (a) opened one or more times; and (b) contained a responsive value in the "company" embedded metadata field.

    b) Crain Report, paragraph 8: Similarly, this analysis determined that at least 255 document instances in the evidentiary population were: (a) opened one or more times; and (b) contained the phrase "Micron confidential."

    The findings in paragraph 9 of the Crain Report, about the document instances opened using Mr. Ho's user profile, are unaffected by any post-seizure access to the devices (or the issue of 2002 date on the BRG010 device).

29. Other than file opening events that occurred post-seizure or were associated with 2002 (with regard to BRG010), the Ashley Disclosure did not address these hundreds of instances where documents were opened that met these criteria, as was detailed in the Crain Report.

IX. The Crain Report Did Not Address Certain USB Devices That Were Connected to Computers Post-Seizure Because No Evidence Was Found Suggesting Those Devices Contained Charged Trade Secret Documents

30. The Crain Report included findings related to three "unrecovered" USB devices, including the forensic evidence indicating these devices contained one or more of the charged trade secret documents.[34] The Ashley Disclosure (at pages 29-30) detailed 10 USB devices that were connected to various computers in this matter on dates/times post-dating the seizure of those computers. And of these 10 USB devices, eight were not provided for analysis by my team or Mr.

[32] *See* Crain Report, ¶¶ 6-9 and Exh. D.
[33] *See* Ashley Disclosure, pp. 22-28.
[34] *See* Crain Report, ¶ 10.

Ashley's team.[35] The Ashley Disclosure then critiques the Crain Report for failing to mention these USB devices that were connected post-seizure. Simply put, the Crain Report did not address these eight USB devices (i.e. that were connected post-seizure, but which were not provided for analysis) because my team and I did not find any evidence indicating that they contained any of the charged trade secret documents (and hence, would not have been a potential source for any of the charged trade secret documents to be copied *on* to the computers).

X. The Ashley Disclosure Includes Additional Incomplete and/or Inaccurate Statements

31. The Ashley Disclosure asserts that the custodian of the BRG014 device was "erroneously list[ed]" in the Crain Report as Ho Jianting (JT Ho), where one documentary source indicates that the device is owned by Kenny Wang.[36] However, while the Ashley Disclosure correctly cites one document, it fails to mention that this information stands in direct conflict with another document, the FBI's Verbatim Translation of the Bill of Indictment of Taichung District Prosecutors Office, Taiwan, which describes the BRG014 device as being "owned by HO Jianting"[37] (capitalization in original).

32. Furthermore, this uncertainty in determining the custodial association of devices is why forensic examiners often analyze the underlying data stored on the device, to 'associate' the device to one custodian or another, even if it cannot confirm legal 'ownership.' The Crain Report included as Exhibit C the analysis performed by my team to attempt to confirm the association of BRG014, which shows multiple independent indicia of the device having been used by JT Ho (including presence of Ho's email on the drive and repeated use of the drive on a computer assigned to Ho and on which Ho – but not Wang – had a user profile). The Ashley Disclosure offers no opinion as to the analysis and findings described in Exhibit C to the Crain Report.

33. The Ashley Disclosure also repeatedly misrepresents the character of files which were "created and then deleted" from various devices. The net effect of the Ashley Disclosure is that the reader is left with the impression that substantive data related to the files in the custodians' possession was added and/or deleted after these devices were seized. Notably, the Ashley Disclosure appears to disregard the critical distinction between a *substantive Microsoft Office file* and the *non-substantive "Office owner" file* (discussed above) that is automatically created and deleted while opening an Office document. In particular:

---

[35] *See* Ashley Disclosure, pp. 29-30.

[36] *See* Ashley Disclosure, p. 19 ("Mr. Crain in his report in *Table 1: List of Frequently Referenced Evidence Items* erroneously lists the Custodian of BRG014 to be Ho Jianting (JT Ho), when the table in Exhibit 2, Page 51 to the Micron Complaint clearly lists the owner of the device as Kenny Wang."); *see also* Ex. 2, Page 51 to the Micron Complaint (the Indictment Decision of Taiwan Taichung District Prosecutors Office, describing a "USB (Kingston brand)" which is "[o]wned by Kenny Wang" and whose "electronic records" were stored "under USB \106030-25-14\").

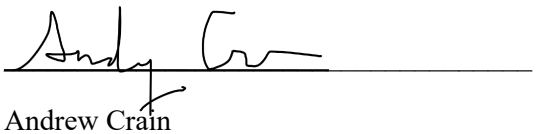
[37] *See* FBI's Verbatim Translation of the Bill of Indictment of Taichung District Prosecutors Office, Taiwan, at p. 35, describing a "Mobile disk (Kingston brand)" that "is owned by HO Jianting" and whose "electromagnetic records are stored in \106030-25-14\").

a) Page 12 of the Ashley Disclosure describes the review of materials on BRG006 on 2/13/2017 which resulted in the "creat[ion] and then delet[ion of] the file titled Fab11_twr_materials_for_25nm_task_force_V6.pptx." However, the file called 'Fab11_twr_materials_for_25nm_task_force_V6.pptx' was neither created on 2/13/2017 on BRG006, nor was it deleted at any point – it is still active on the device.[38] The file created and deleted on the device on 2/13/2017 was only the small non-substantive "Office owner" file called "~$Fab11_twr_materials_for_25nm_task_force_V6.pptx."[39]

b) Page 18 of the Ashley Disclosure makes the same allegation that a specific file on BRG013 being reviewed by the MJIB "is the file that was created and then deleted" during examination.[40] However, the substantive file Mr. Ashley described was not created or modified on the device post-seizure, nor was it deleted at any point; only the small non-substantive "Office owner" file was created and deleted.[41]

c) Page 19 of the Ashley Disclosure makes the same allegation as to two specific files on BRG014 being reviewed by the MJIB as "two of the files where were created and then deleted from the device."[42] However, the two substantive files Mr. Ashley discussed were not created or modified on the device post-seizure, nor were they deleted at any point; only the small non-substantive "Office owner" files were created and deleted.[43]

Dated: October 15, 2021



Andrew Crain

[38] *See* Ashley Disclosure, Exh. 10 (showing file was created 1/15/14 19:00 and not deleted).
[39] *Id.*
[40] *See* Ashley Disclosure, p. 18 ("It is apparent from the transcript of the MJIB interrogation of the Micron employee Yi-Leng Chen that he actually reviewed the files and folders on this device which had their metadata altered. In his answer at the bottom of page 4 of the interrogation transcript he **specifically references the file \4GLP2\WT\4GMLP2A_Category_Bin_define_Ver0A (Non-C-comp)_vl.xlsm, which is the file that was created and then deleted from the device**.") (emphasis added).
[41] *See* Ashley Disclosure, Exh. 16 (which does *not* list the file "4GMLP2A_Category_Bin_define_Ver0A (Non-C-comp)_vl.xlsm," because that file was not created or modified after seizure, but does list the corresponding "Office owner" file "~$4GMLP2A_Category_Bin_define_Ver0A(Non-C-comp)_v1.xlsm").
[42] *See* Ashley Disclosure, p. 19 ("It is apparent from the transcript of the MJIB interrogation of Micron employee Yi-Leng Chen that he actually reviewed the files and folders on this device which were created and then deleted from the device. In his answer at the bottom of page 4 and the top of page 5 of the interrogation transcript he **specifically references the files DRAM data\DRAM flow data\cell dummy\ECD-2013000667-001_25nmS_6F2_MemoryCel.ppt (*sic*) and80series_dram_overview_and_comparison.pptx (*sic*) which are two of the files which were created and then deleted from the device**.") (emphasis added; errors in original).
[43] *See* Ashley Disclosure, Exh. 17 (which does *not* list either file, because neither file was created or modified after seizure, but does list the corresponding "Office owner" files "~$ECD-2013000667-001_25nmS_6F2_MemoryCell.ppt" and ~$80series_dram_overview_and_comparison.pptx")